AMENDMENTS TO THE SPECIFICATION AND ABSTRACT

Please amend the paragraph [0018] beginning on page 8 as follows:

[0018] [FIG. 1] FIG. 1 shows a general structure of a wireless LAN system according to a first embodiment of the present invention.

[FIG. 2] FIG. 2 is a sequence diagram showing a basic authentication procedure performed between two parties.

[FIG. 3] FIG. 3 is a flowchart showing processing of an authentication method according to the first embodiment of the present invention.

[FIG. 4A] FIG. 4A shows an example of an authentication request.

[FIG. 4B] FIG. 4B shows an example of an authentication response.

[FIG. 5A] FIG. 5A shows an example of a display screen of a display section 13.

[FIG. 5B] FIG. 5B shows an example of a display screen of the display section 13.

[FIG. 6] FIG. 6 is a sequence diagram showing an authentication procedure performed between three parties.

[FIG. 7] FIG. 7 shows an example of a display screen of the display section 13.

[FIG. 8] FIG. 8 is a sequence diagram showing an authentication procedure performed when an illegal party exists between two parties.

[FIG. 9] FIG. 9 shows a general structure of a wireless LAN system according to a second embodiment of the present invention.

[FIG. 10] FIG. 10 is a sequence diagram showing a basic authentication procedure performed between two parties.

[FIG. 11] FIG. 11 is a flowchart showing processing of an authentication method according to the second embodiment of the present invention.

[FIG. 12A] FIG. 12A shows an example of an authentication request.

[FIG. 12B] FIG. 12B shows an example of an authentication response.

[FIG. 12C] FIG. 12C shows an example of a key generation request.

[FIG. 12D] FIG. 12D shows an example of a key generation response.

[FIG. 13] FIG. 13 is a sequence diagram showing an authentication procedure performed between three parties.

[FIG. 14] FIG. 14 is a sequence diagram showing an authentication procedure performed when an illegal party exists between two parties.

[FIG. 15] FIG. 15 shows an exemplary detailed structure of authentication sections 12 and 22.

[FIG. 16] FIG. 16 is a flowchart showing processing of an authentication method according to a third embodiment of the present invention.

[FIG. 17] FIG. 17 shows an example of a format of an authentication request message.

[FIG. 18] FIG. 18 shows an example of a format of an authentication response message.

[FIG. 19] FIG. 19 shows an example of a format of an authentication request message which has been changed and forwarded.

[FIG. 20] FIG. 20 shows an example of a format of an authentication response message which has been changed and forwarded.

[FIG. 21] FIG. 21 shows an example of a format of an authentication response message.

[FIG. 22] FIG. 22 shows an example of a format of an authentication response message which has been changed and forwarded.

[FIG. 23] FIG. 23 shows an example of a format of a common encryption key generation request message.

[FIG. 24] FIG. 24 shows an example of a format of a common encryption key generation response message.

[FIG. 25] FIG. 25 is a sequence diagram showing an authentication procedure performed in a wireless LAN system according to another embodiment.

[FIG. 26] FIG. 26 is a sequence diagram showing an authentication procedure performed in a wireless LAN system according to still another embodiment.

[FIG. 27] FIG. 27 is a sequence diagram showing an operation procedure by which APs share ID information of a client.

[FIG. 28] FIG. 28 is a sequence diagram showing an authentication procedure performed between an AP and the client when the APs share the ID information of the client.

[FIG. 29] FIG. 29 is a sequence diagram showing an authentication procedure ~~performed when APs share the ID information of the client~~ by which the ID information of the client is shared by all the APs in a decentralized manner.

[FIG. 30] FIG. 30 is a sequence diagram showing an embodiment in which the ID information of the client is shared using a router.

[FIG. 31] FIG. 31 is a sequence diagram showing an authentication procedure performed in the embodiment in which the ID information of the client is shared using the router.

[FIG. 32] FIG. 32 is a sequence diagram showing an operation of erasing authenticated ID information of a client by connection disruption.

[FIG. 33] FIG. 33 is a sequence diagram showing an operation of erasing authenticated ID information of a client stored in a plurality of APs by connection disruption.

[FIG. 34] FIG. 34 is a sequence diagram showing an operation of erasing authenticated ID information of a client stored in the router by connection disruption.

[FIG. 35] FIG. 35 is a flowchart showing an example of processing of a conventional authentication method.

[FIG. 36] FIG. 36 is a flowchart showing an example of processing of a conventional authentication method.

[FIG. 37] FIG. 37 is a flowchart showing an example of processing of a conventional authentication method.

Please amend the paragraph [0025] beginning on page 16 as follows:

[0025] The input section 14 is provided for the user to input data and commands to the master 10 and also to input the determination result on whether or not to verify the authentication based on the display by the display section 13. The input section 24 is provided for the user to input data and commands to the ~~slave 20~~ master 10. The input sections 14 and 24 each include, for example, a push button.

Please amend the paragraph [0026] beginning on page 16 as follows:

[0026] In the wireless LAN system in the first embodiment, only the master 10 includes the display section 13. For example, the slave 20 may be a network camera with no display section, and the master 10 may be a network camera controller with the display section 13. Hereinafter, an authentication procedure performed by the wireless LAN system in the first embodiment will be described. When the authentication sections 12 ~~13~~ and 22 ~~23~~ are mounted on a MAC layer, the messages exchanged between the master 10 and the slave 20 may be in a known format of, for example, the MAC layer standard of IEEE Standard 802.11.

Please amend the paragraph [0039] beginning on page 16 as follows:

[0039] (1) Basic authentication procedure performed between two parties (FIG. 10)

For performing authentication with the master 40, the slave 50 transmits an authentication request to the master 40 (step S1111). FIG. 12A shows an example of the authentication request. The master 40 receives the authentication request (step S1101), and transmits an authentication response which includes device information including its own ID and public key (or electronic signature) to the slave 50 (step S1102). FIG. 12B shows an example of the authentication response. The slave 50 receives the authentication response (step S1112), and displays the device information included in the authentication response ~~request~~ on the screen of the display section 23 (step S1113). The display screen of the display section 23 is as the examples shown in FIG. 5A and FIG. 5B. The user visually checks the device information displayed on the screen of the display section 23, determines whether or not to verify the authentication, and instructs the slave 50 of the determination result via the input section 24 (step S1114). This instruction is typically performed by pushing a push button. The slave 50, instructed to verify or not to verify the authentication, performs the processing in accordance with the instruction.

Please amend the paragraph [0044] beginning on page 26 as follows:

[0044] (3) Authentication procedure when an illegal party exists between two parties (FIG. 14)

The slave 50 transmits an authentication request to the master 40. In response to the authentication request, the master 40 transmits an authentication response including device information [ID1, key1] to the slave ~~50~~ 40. However, the authentication response does not reach the slave 50 and is received by an illegal party device 90. The illegal party device 90 transmits, to the slave 50, an authentication response including pseudo device information [ID1, key2], which replaces the device information [ID1, key1] in order to disguise the illegal party device 90 as the master. The slave 50 receives the authentication response and displays the device information included in the authentication response on the screen of the display section 23. The user visually checks the device information displayed on the screen of the display section 23 and determines that the public key information of the displayed device information does not match that of the device information of the master 40 to be authenticated. Namely, the user recognizes that the displayed device information [ID1, key2] is different from [ID1, key1], which is of the device information of the master 40 already obtained. In accordance with the determination, the user terminates the authentication process. Substantially the same procedure is usable in the case where an electronic signature is used for the device information instead of the key.

Please amend the paragraph [0052] beginning on page 33 as follows:

[0052] When the authentication request 1603 is successful, an authentication response 1605 is returned from the AP 10 to the client 20. An example of the format of the authentication response 1605 is shown in FIG. 18. A PLa 1802 includes an authentication result. A PKa 1804 is a public key of the AP 10. An IDa 1803 is an ID of the AP 10. A SIGNa 1805 is a signature made for each field of the authentication response 1605 using the secret key and the electronic signature of the AP 10. The transmission/reception section 11 of the AP 10 obtains the public key PKa 1804 of the AP 10 ~~client 20~~ from the public key/secret key generation section 111. The transmission/reception section 11 also obtains the SIGNa 1805 from the electronic signature section 112, and assembles the SIGNa 1805 with the IDa 1803 owned by the authentication section 12 ~~21~~ to generate the authentication response 1605. The authentication response 1605 allows the public key PKa 1804 of the AP 10 to be transferred to the client 20.

Please amend the paragraph [0055] beginning on page 34 as follows:

[0055] (Second Specific Example)

The client 20 or the AP 10 monitors whether or not the authentication request message is changed and transferred by a man-in-the-middle device. In the case where the client 20 can receive all the messages transmitted by man-in-the-middle devices, it is effective that the client 20 performs the monitoring. In the case where the AP 10 can receive all the messages transmitted by the client 20 and all the messages transmitted by man-in-the-middle devices, it is effective that the AP 10 performs the monitoring. In the case where the client 20 monitors, the client 20 affirms that an act of changing and forwarding has been conducted by a man-in-the-middle device when an authentication request, which is received before an authentication response is returned from the AP 10 to the client 20, matches the authentication request transmitted by the client 20 itself except for the public key and the signature included therein. In the case where the AP 10 monitors, the AP 10 affirms that an act of changing and forwarding has been conducted by a man-in-the-middle device when the AP 10 receives two authentication requests which are exactly the same except for the public key and the signature within a predetermined time period. When the AP 10 receives an authentication request ~~response~~ 402 as shown in FIG. 19, that means either that the AP 10 receives two authentication requests ~~responses~~ which are the same except for the public key PKm 1904 and the signature SIGNm 1905, or that the client 20 also receives the authentication request having the public key and the signature replacing those of the authentication request transmitted by the client 20 itself. In either case, it can be affirmed that an act of changing and forwarding has been conducted by a man-in-the-middle device.

Please amend the paragraph [0061] beginning on page 38 as follows:

[0061] When the AP 10 accurately receives the common encryption key generation request 1606 and confirms the authenticity thereof, the AP 10 returns a common encryption key generation response 1607 shown in FIG. 24 to the client 20. The common encryption key generation response 1607, except for a header HDRa 2401, is encrypted using the public key PKc of the client 20. An IDa 2402 is an ID of the AP 10. A Na 2403 is a random number generated by the AP 10. The encryption section 113 of the AP 10 obtains and encrypts an IDa retained by the transmission/reception section 11 of the AP 10 and the random number Nc generated by the pseudo random number generation section 115 of the AP 10. The transmission/reception section 11 of the AP 10 adds the header HDRa 2401 to the encrypted IDc and random number Na, and transmits the resultant common encryption key generation response 1607. The transmission/reception section 21 of the client 20 receives the common encryption key generation response 1607, and retrieves and transfers data to be decrypted to the decryption section 114. The decryption section 114 decrypts the data by its own secret key. With the decryption result, it is confirmed that the ID is the IDa of the AP 10 authenticated before. In the case where this is confirmed, the client 20 keeps the ~~random number~~ Na obtained in the decryption result to be used for key generation later. Otherwise, the received common encryption key generation response 1607 is discarded and key generation is cancelled.

Please amend the paragraph [0073] beginning on page 44 as follows:

[0073] In order to permanently separate the client from the network, as shown in FIG. 32, the client 20 transmits a disconnection message 3202 with its own ID to the AP 10. The AP 10, which has received the disconnection message 3202, deletes the ID information of the client 20 from its own database by a procedure 3203. All is needed to realize this is that the client 20 is set so as to transmit a disconnection message to AP 10 when the user selects to disrupt the connection, so that the ID information of the client 20 is erased from the authenticated ID information stored in the devices in the network.

Please amend the paragraph [0074] beginning on page 45 as follows:

[0074] In the case of the AP sharing system or the AP decentralized management system by which other APs other than the AP 10 share the authenticated ID information, as shown in FIG. 33, the AP 10 which has received a disconnection message 3302 notifies the authenticated ID information to be erased to the APa's by a multicast disruption message 3303 to request the erasure of the authenticated ID information, and the APa which has received the erasure request erases the authenticated ID information when storing such ID information. The AP 10, which first received the disconnection message 3302, also erases the ID information of the client 20 as the authenticated ID information by a procedure 3304 when storing such ID information. After erasing the authenticated ID information, the APa returns a disconnection response message 3306 to the AP 10. Then, the AP 10 returns a disconnection response message 3307 to the client 20.